Exhibit 3

FBI admitted attack against the Freedom Hosting

September 16, 2013 By Pierluigi Paganini

IT'S CLEAR

In an Irish court the FBI Supervisory Special Agent Donahue revealed that FBI had control of the Freedom Hosting company to investigate on child pornography.

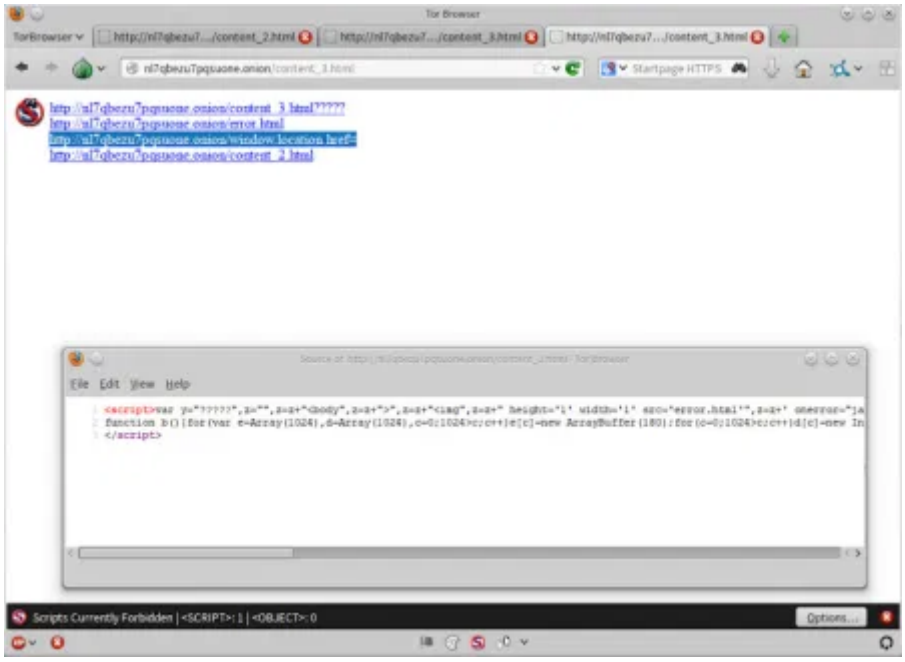
FBI admitted publicly that the Bureau had compromised the Freedom Hosting, probably the most popular Tor hidden service operator company.

The news confirms the suspects raised after that a group of Security researchers found a malicious script that takes advantage of a Firefox Zero-day to identify some users of the Tor anonymity network.

In an Irish court the FBI Supervisory Special Agent Brooke Donahue revealed that the FBI had control of the Freedom Hosting company to investigate on child pornography activities, Freedom Hosting was considered by US law enforcement the largest child porn facilitator on the planet.

event and reloading of pages could sometimes cause a crash when unmapped memory is executed. This crash is potentially exploitable."

The exploit is based on a Javascript that is a tiny Windows executable hidden in a variable dubbed "***Magneto***". Magneto code looks up the victim's Windows hostname and MAC address and sends the information back to the FBI Virginia server exposing the victims's real IP address. The script sends back the data with a standard HTTP web request outside the Tor Network.



Eric Eoin Marques, the 28-year-old Irishman owner and operator of Freedom Hosting**,** is now awaiting extradition to the US where he could face 100 years in prison on child pornography charges. The new details emerged in press reports from a Thursday bail hearing in Dublin, where Marques, 28, is fighting extradition to America on the above charges. He was denied bail for the second time since his arrest in July. According law enforcement Marques might reestablish contact with co-conspirators, and further complicate the FBI probe.

Freedom Hosting hosted hundreds of discutible websites, many of them used to conduct illegal activities taking advantage of the anonymity provided by Tor network. Tor network contains in fact many services that are used by cyber criminals for money laundering, exchanging of child porn material, renting for hacking services and sale of drugs and weapons.
Freedom Hosting offers hosting services to hacking sites such as HackBB and at least 550 servers throughout Europe that distributed child porn content.Donahue revealed that the Freedom Hosting service hosted at least 100 child porn sites providing illegal content to thousands of users, and claimed Marques had visited some of the sites himself.

Eric Eoin Marques knew he hunted, apparently he already sent the earnings to his girlfriend over in Romania, the FBI is analyzing the Marques's seized computer discovered that he had made inquiries about how to get a visa and entry into Russia, and residency and citizenship in the country. Marques's made also searches for a US passport template and a US passport hologram star, probably he was planning an escape. In 2011 the group of hacktivist Anonymous also attached the F

reedom Hosting with a series of DDoS attacks after allegedly finding the firm hosted more that 90% of the child porn hidden services on the Tor network. Court documents and FBI files released under the FOIA have described the CIPAV (Computer and Internet Protocol Address Verifier) as software the FBI can deliver through a browser exploit to gather information from the suspect's machine and send it to on the server of the Bureau in Virginia.

The event is the confirmation that Tor network provides an extra layer of obfuscation but it must be clear it does not provide bulletproof online anonymity, various researches already that evidenced it.

Pierluigi Paganini

(Security Affairs – Tor, cybercrime, Freedom Hosting)

Share this:

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
CBMEN, DARPA’s peer-to-peer technology for battlefield

NEXT ARTICLE
Hacking - Give me 10 minutes to hack the Nasdaq

YOU MIGHT ALSO LIKE

European Council extends sanctions against foreign threat actors

May 18, 2021 By Pierluigi Paganini

Analysis of NoCry ransomware: A variant of the Judge ransomware

May 18, 2021 By Pierluigi Paganini